Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2015, *9*, 2709-2717

Open Access

The Prediction Model of Dynamic Trust Relationship based on the Influence of Fuzzy Weight

Li Qiang[1,*], Wang Yuanyuan[2] and Niu Wensheng[3]

[1]*School of Computer Science and Technology, Xidian University, Shaanxi Xi'an, 710071, P.R. China;*

[2]*Social Science Department, Xi'an Peihua University, Shaanxi Xi'an, 710065, P.R. China;*

[3]*AVIC Xi'an Aeronautics Computing Technique Research Institute, Shaanxi Xi'an, 710068, P.R. China*

Abstract: The establishment of trust-relationships, in a sense, averts the potential dangers which caused by the aimless interaction between entities. This paper proposes the technical route and the complete prediction model for the dynamic trust-relationships prediction aims at the limitation of historical evidence and the dynamic nature of trust-relationships. This model can do screening for malicious recommendation and wrong recommendation, and encourage or punish the historical trust degree by means of fuzzy weight, fully reflect the importance of weight upon the dynamic nature of the model and the essential characteristics of trust-relationships between entities. This model, whose algorithm bears better convergence and expansibility, does not possess complicate computation.

Keywords: Fuzzy weights, dynamic trust, trust degree, trust-relationships prediction, malicious recommendation, wrong recommendation.

1. INTRODUCTION

Since 1996, Blaze *et al*. [1] put forward the concept of trust management for the first time, many scholars have put forward a variety of trust relationship model in the open environment [2-18]. These models reflect the dynamics and uncertainty of trust relationship from different aspects, and promote the development of the trust relationship theory effectively. Although many useful conclusions have been drawn from the former research, there still exist a lot of risks and uncertainties combining with the complexity of the trust issue make the establishment of the trust relationships between entities very difficult in the dynamic environment. Some problems still exist.

1) Take the trust relationship isolated. There is a connection between the direct and indirect trust relationships between entities. It could not take either of those as the unique determinant of trust reasoning. The result of direct trust and indirect trust should be consistent after excluding the malicious recommendation and error recommendation. Separating the relations between those two randomly is inappropriate.

2) Assume the limitations of large sample data. Basic descriptions of trust in the existing models are based on a hypothesis that the evidence on the basis of the past is sufficient. But we do not have a lot of data for our reference in many cases. In the small samples case, the traditional statistical theory under the support of trust models is likely to lead to incorrect results.

3) Insufficient understanding of the dynamics of trust. The multiple trust evaluations from trust subject to trust object are not single value without connection. They should match some kind of distribution. This distribution could adapt to the nature of trust relationship by fitting a specific environment and foundation.

Trust relationships belong to the category of human psychological cognition. It is inevitably acceptable that the evolution of the trust relationships between entities do not conform to the human psychological cognitive process of trust. Trust is established on the historical interaction evidence, and the historical evidence is constant. Modeling must give full expression to this depends on dynamic characteristics of the trust relationship which based on the constant of historical evidence. Also, these historical evidences have been discriminated by emphasis degree. Based on the above ideas, this paper puts forward the prediction model of dynamic trust relationship based on the influence of fuzzy weight

2. PROBLEM MODEL AND TECHNICAL ROUTE

The definition of some related concepts presented first before building the problem model and determining the technical route.

1874-110X/15

Definition 1 Entity Role

According to the different roles of entities in the open environment, this paper defines three types of entity role: the Service Provider (SP), the Service Requestor (SR) and Feedback Rater (FR).

In the definition of three kinds of roles, SP is trust subject (namedTrustor), SR is trust object (named Trustee), and FR is respondent entity. SP grade the service which provided by itself according to the sensitivity, and regulate SR can obtain corresponding level of service only satisfy a certain trust degree. When SR request service to SP, SP makes comprehensive judge in accordance with the direct trust to SR and feedback trust degree of FR. Then provide service to the SR on the basis of former result. The entities involved in this paper belong to one of the three types of entities role in one interaction.

Definition 2 Direct Trust Degree (DT)

Direct Trust Degree is the trust degree one entity to another according to the historical record of the direct interaction in the context. Assuming the entity collection $\boldsymbol{P} = \{P_1, P_2, \dots, P_n\}$, $DT(P_i, P_j)$ is the direct trust degree of entity P_i （SP） to entity P_j （SR） , noted DT_{ij}, and $DT_{ij} \in [0,1]$.

Definition 3 Feedback Trust Degree (FTD)

The relationship between trust subject$P_i$and trust object P_j is established by feedback information of FR. Assuming FR collection is $\boldsymbol{E} = \{e_1, e_2, \dots, e_l\}$, $FTD(P_i, P_j, e_k)(k = 1,2, \dots, l)$ is the feedback trust degree oftrust subject P_i totrust object P_j on the basis of the feedback information of entity FR, and $FTD(P_i, P_j, e_k) \in [0,1]$. Feedback trust degree referred as indirect trust degree or recommend trust degree.

Definition 4 Overall Trust Degree (OTD)

Overall Trust evaluation to trust object P_j is formed after trust subject P_i gathered the direct trust and all effective feedback trust. $OTD(P_i, P_j)$ refers to the overall trust degree of trust subject P_i and trust object P_j,$OTD(P_i, P_j) \in [0,1]$. Overall Trust Degree also known as the global trust degree.

Definition 5 Entity Credit Worthiness (CW)

Credit Worthiness of an Entity is the inherent nature of the Entity. It is an objective reality. To most of entities, it refers the trust degree of. Assume CW_jisthe credit worthiness of entity P_j, $CW_j \in [0,1]$.

Obviously, the overall Credit Worthiness of trust subject P_i to trust object P_j is

$$OTD(P_i, P_j) = f\left(DT(P_i, P_j), g_{k=1}^{m}\left(FTD(P_i, P_j, e_k)\right)\right) \quad (1)$$

It is a function of Direct Trust Degree $DT(P_i, P_j)$ and Feedback Trust Degree $FTD(P_i, P_j, e_k)$, and

$$g_{k=1}^{m}\left(FTD(P_i, P_j, e_k)\right) \quad (2)$$

is an aggregate function of Feedback Trust Degree $FTD(P_i, P_j, e_k)(k = 1,2, \dots, m)$, m is valid entity number of FR.

Feedback trust degree $FTD(P_i, P_j, e_k)$ is a function of $DT(P_i, e_k)$ and $DT(e_k, P_j)$

$$FTD(P_i, P_j, e_k) = \phi\left(DT(P_i, e_k), DT(e_k, P_j)\right) \quad (3)$$

Fig. (**1**) shows the conceptual model of Dynamic trust relationship prediction problem (Regardless of the multi-stage feedback).

Sociology experience shows that the longer of the interaction history, the more of the interaction frequency, the higher of familiarity degree, and the easier to establish a trust relationship. This phenomenon reflects the time aggregation that direct trust relationship to the interact history. Most of the existing models recognize the importance of direct trust. When direct trust evidence is insufficient, the judgment will be made according to the feedback of FR. Using FR feedback to establish trust based on the following four aspects:

1) If the Trustor and the Trustee never interacted, FR feedback is required to help the Trustor and the Trustee to establish a trust relationship.
2) If the Trustor and the Trustee had few interactions or have no interaction with each other for a long time until now, the Trustor requires the feedback information of FR to redo the judgment.
3) Due to the change of environment, the Trustor need to re-assessment the trust evaluation to Trustee (determined by the security policy), the Trustor also need the feedback information of FR to judge.
4) In consideration of the importance of affairs and the Trustors' personal preference, Trustordoes not be confident to itself. It needs the feedback information of FR to help establish the trust relationship to Trustee.

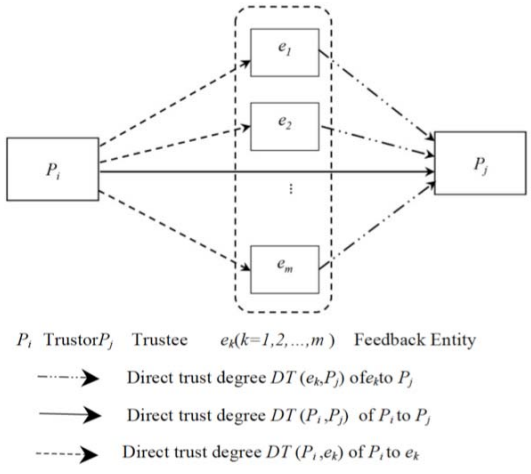

Fig. (1). The conceptual model of Dynamic trust relationship prediction problem.

Fig. (**2**) shows the technical routed of dynamic trust relationship prediction of this paper:

1) If P_i and P_j had several interactions and had interact request behavior recently, calculate the $DT(P_i, P_j)$ firstly and judge whether $DT(P_i, P_j) \geq \alpha$ is established according to the direct trust aggregation algorithm. α is the trust threshold and the average value of it is less than 0.3, which is determined by the actual demand. If $DT(P_i, P_j) < \alpha$, then $OTD(P_i, P_j) = DT(P_i, P_j)$. It means P_i have sufficient reason to refuse interaction request of P_j. Otherwise, turn to next step.

2) Determine whether $DT(P_i, P_j) \geq \beta$is established. β is direct trust threshold and the average value is more than 0.9.If $DT(P_i, P_j) \geq \beta$, then $OTD(P_i, P_j) = DT(P_i, P_j)$. It means that P_i is very familiar with P_j. There is sufficient reason to consider P_j is very credible without the feedback information of FR, and the interactive request could be established. Otherwise, turn to next to step. Steps 1 and 2 fully show the importance of direct trust relationship, as shown in Fig. **2**①.

3) When $\alpha \leq DT(P_i, P_j) < \beta$, P_i accept the trust feedback information from entity FR toP_j. Assuming the number of FR entities is l, they are $e_k(k = 1,2, \dots, l)$. Firstly, determine whether $DT(P_i, e_k) \geq \gamma$ is established. γ is feedback trust threshold and the average value is large than 0.7. That is to say, P_i would trust the recommend information from respondents only when it fully trust the respondents. Otherwise, it will refuse to accept recommendation information from low trust entity. Through this step, malicious recommendation from the malicious entities could be got rid to a large extent. As shown in Fig. **2**②.

4) When $DT(P_i, e_k) \geq \gamma$, calculate $FTD(P_i, P_j, e_k)$. Namely establish the feedback trust degree from P_i to P_j according to the feedback information of FR entitye_k.

5) P_i filter out the error recommendation from FR entity and accept effective feedback trust information from FR to do the trust evaluation for P_j, as shown in Fig. **2**③. Assuming the number of effective FR entities which could accept is m, it means m recommends from respondents $e_k(k = 1,2, \dots, m.\ m \leq l)$. Finally, calculate the overall trust degree of P_i and P_j according to the formula (1).

3. PREDICTION MODEL OF DYNAMIC TRUST RELATIONSHIP

3.1. The Computation of Direct Trust Degree

The direct trust relationships between entities are entirely determined on the basis of past experience of direct interaction.

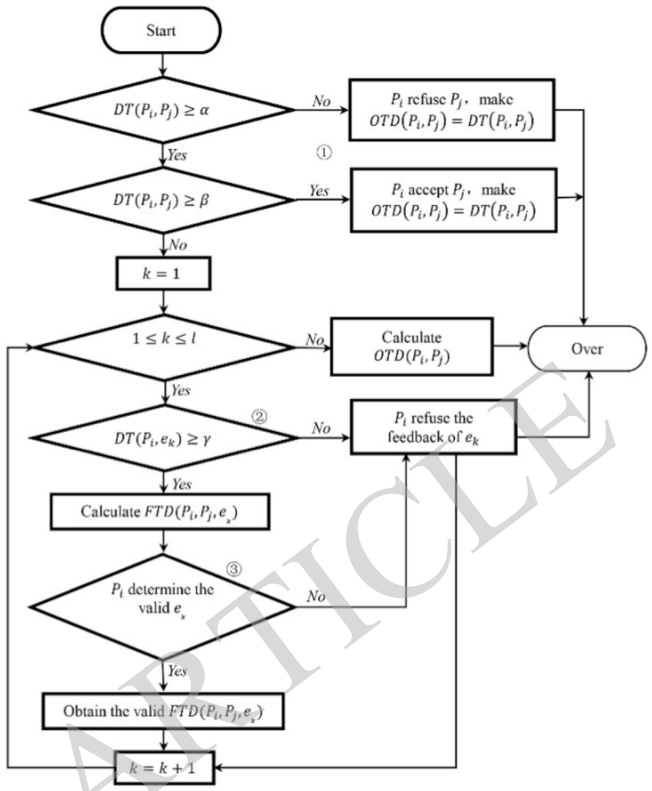

Fig. (2). Technical routed of dynamic trust relationship prediction.

Definition 6 Direct Trust Degree Aggregation Algorithm

Assuming the collection of trust degree evaluation between trust subject P_i and trust object P_j produced in the recent h time interactive process is $\boldsymbol{DT} = \{DT_{ij}^{(1)}, DT_{ij}^{(2)}, \dots, DT_{ij}^{(h-1)}, DT_{ij}^{(h)}\}$. $DT_{ij}^{(k)}$ represents the trust degree of the kth interaction of P_i and P_j,$DT_{ij}^{(k)} \in [0,1]$, $k = 1, 2, \dots, h$. The trust degree evaluation data is ranked according to the order of interactiontime, $DT_{ij}^{(1)}$ represents an interaction long time ago, $DT_{ij}^{(h)}$ represents a recent interaction. The direct trust from P_i to $P_j$is defined as:

$$DT(P_i, P_j) = DT_{ij} = \begin{cases} \sum_{k=1}^{h} w(k) DT_{ij}^{(k)}, & h \neq 0 \\ 0.5 \text{ or } CW_j, & h = 0 \end{cases} \quad (4)$$

$w(k)$is the weight of trust degree $DT_{ij}^{(k)}$ in the kth interaction, and $w(k) \geq 0\ (k = 1, 2, \dots, h) \sum_{k=1}^{h} w(k) = 1$. CW_j is the credibility of trust object P_j.

Obtain the weight sequence $\{w(k)\}\ (k = 1, 2, \dots, h)$ by establishing the Minimum variance programming model [19]. The weight of minimum variance of time series can be obtained [20].

$$w(k) = \frac{(6h-12k+6)\alpha - 2h + 6k - 2}{h(h+1)}, k = 1,2, \dots, h \quad (5)$$

In this formulation:

$$\frac{h-2}{3h-3} \leq \alpha < \frac{1}{2} \quad (6)$$

Here $w(k+1) > w(k)$, $k = 1,2,\dots,h-1$. It means the sequence $\{w(k)\}$ is monotone increasing time sequence. It matches the characteristics of social psychology and behavioristic of the trust relationship. It indicates that people always give greater weight to new interaction and the trust relationship dynamically attenuates with the time (the longer interval is, the contribution of previous trust value to evaluate the present trust relationship lessis). Restricted by the formula (6), by giving α, the orness measure levels, different values. Different weight sequence with various distribution can be obtained. It could control the degree of the attention (or oblivion) of the previous historical evidence effectively to make flexible choice under the dynamic environment. At the same time, the weight sequence $\{w(k)\}\,(k = 1,2,\dots,h)$ has the following character:

$$w(k+1) - w(k) = \frac{6-12\alpha}{h(h+1)} > 0, \quad k = 1,2,\dots,h-1 \qquad (7)$$

$\{w(k)\}\,(k = 1,2,\dots,h)$ is an increasing arithmetic sequences. When α and h is fixed, the difference of adjacent weight coefficient is irrelevant with k, the distance of the adjacent weight coefficient is equal. It has good linear characteristic and dynamic adaptability without complex iterative process. Also the calculation is simple and it has good scalability.

3.2. The Calculation of Feedback Trust Degree and Selection of Effective Feedback Trust Degree

There are two values associated with feedback trust: $DT(P_i, e_k)$ and $DT(e_k, P_j)$. In theory, feedback trust degree $FTD(P_i, P_j, e_k)$ match the character of T triangle modulus. That reflects relative trust got lost in the transfer process during the polymerization of feedback trust relationship. Any improvement of direct trust will improve the characters such as feedback trust degree. This article use real multiple computing, namely:

$$FTD(P_i, P_j, e_k) = \phi\left(DT(P_i, e_k), DT(e_k, P_j)\right)$$
$$= DT(P_i, e_k) \times DT(e_k, P_j) \qquad (8)$$

In the process of establishing the feedback trust relationship, removing the malicious entities is based on setting the feedback trust threshold γ. In addition, even though every feedback entity is well-meaning, it is hard to ensure well-meaning feedback entities will present absolutely accurate feedback information. At the same time, different well-meaning feedback entities will present different feedback information. Theoretically, the trust degree that Trustor to Trustee will present a certain stability in a period with the frequent interaction of them and the more participation of Trustor. The trust degree would gradually converge to the Trustee's credibility. So, after malicious or error feedback been blocked, either directly trust relationship evaluation or feedback trust evaluation should be distributed near the credibility of Trustee. Or, most of feedback information should be consistent. It's hard to trust a respondents whose feedback information deviate from the majority. However, the truth is the Trustor would receive a lot of error recommends from credible respondents, and then have deviation on the trust evaluation of Trustee. Therefore, the distribution of the feedback information should be further studied. Filter the feedback information which would seriously deviate the credibility of Trustee and keep effective information to be used in the overall evaluation of trust relationship.

In the open network environment, the feedback information received by different Trustor received has much uncertainty. It mainly reflected in the variable number of FR entity, variable size of feedback information and complex distribution (mixture distribution or unknown distribution). In this situation, using the statistical to research would not get a good conclusion. Considering the complexity and fuzziness of feedback trust, this paper uses non-statistical estimation method based on fuzzy set theory [21] to estimate the unknown distribution of feedback information.

Assuming the feedback information Trustor received which from FR entity to Trustee trust is:

$$\boldsymbol{FTD} = \{FTD(P_i, P_j, e_1), \dots, FTD(P_i, P_j, e_l)\} \qquad (9)$$

Formula (9) can be shorthand for:

$$\boldsymbol{FTD} = \{FTD_{ij}^{(1)}, FTD_{ij}^{(2)}, \dots, FTD_{ij}^{(l)}\} \qquad (10)$$

$FTD_{ij}^{(k)}$ is equivalent to $FTD(P_i, P_j, e_k)(k = 1,2,\dots,l)$. The sample size of this kind of non-statistical estimation method can be less to four, and there is no requirement for the data distribution. As long as $l \geq 4$, there will be a very good estimate effect, and when l is bigger, the results of this method and the result of statistical method are basically the same.

This method adopts the sort linear estimation [22] to obtain the distribution of the feedback trust degree. In Fig. (**3**), FTD_0 is the true value of population distribution of FTD. Theoretically, it could be estimated according to the principle of maximum membership degree [22]. FTD_L is the lower bound of FTD population distribution, and FTD_U is the upper bound.Using the maximum minimum model method to estimate and the approximation error is less than that of the classical least square method. The estimation of the FTD population distribution is:

$$FTD \in [FTD_0 - \delta_L, FTD_0 + \delta_U] = [FTD_L, FTD_U] \qquad (11)$$

λ is the optimal level. In fuzzy set theory, $\lambda = 0.5$. It means the most uncertain case, the most ambiguous situation. The strict mathematical analysis and derivation to this algorithm can be referenced from [21]. When $\lambda \geq 0.5$, it indicates the collection $[FTD_L, FTD_U]$ contains all useful FTD. This is the effective feedback trust degree we are looking for which distribute around the trust degree of Trustee (estimated value is FTD_0). After reasonable aggregation, the valid FTD is used in the overall trust computing with direct trust degree. The FTD which distributed at the outside of $[FTD_L, FTD_U]$ and far away from FTD_0. They are considered wrong to recommend and should be rejected.

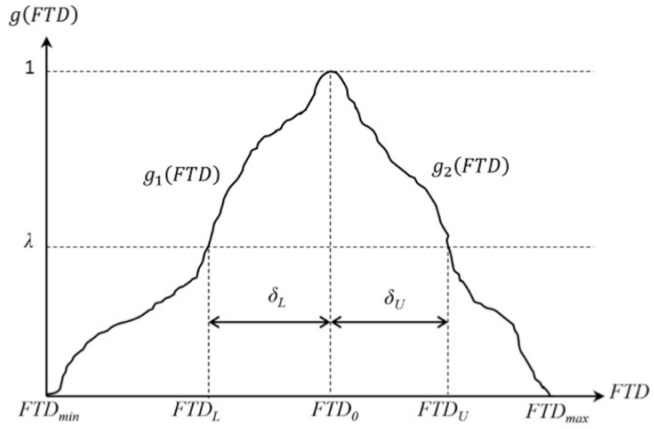

Fig. (3). The distribution of FTD (subordinate function).

3.3. Aggregation of Feedback Trust Degree

Make aggregation for the feedback trust degree which has been eliminated the malicious recommendation and the error recommendation, the Trustor has formed the effective feedback evaluation to the Trustee.

Definition 7 Feedback Trust Degree Aggregation Algorithm

Assuming the Feedback Trust sequence Trustor accepted to from the effective FR entity to the Trustee is:

$$\boldsymbol{FTD} = \{FTD(P_i, P_j, e_1), \dots, FTD(P_i, P_j, e_m)\} \quad (12)$$

Shorthand for formula (12):

$$\boldsymbol{FTD} = \left\{FTD_{ij}^{(1)}, FTD_{ij}^{(2)}, \dots, FTD_{ij}^{(m)}\right\} \quad (13)$$

The feedback trust degree after aggregation is as follows:

$$g_{k=1}^{m}\left(FTD_{ij}^{(k)}\right) = \sum_{k=1}^{m} \omega_k \times FTD_{ij}^{(k)} \quad (14)$$

ω_k is the weight of feedback trust degree $FTD_{ij}^{(k)}$ $(k = 1,2, \dots, m)$.

It can be seen from the formula (14) that the feedback trust degree after aggregation can be calculated as long as the weight ω_k $(k = 1,2, \dots, m)$ be determined. Take two aspects into account to determine the weight ω_k $(k = 1,2, \dots, m)$:

1) Determine the Weight According to the Distribution of FTD

Known from the analysis above, most feedback trust FR entity to the Trustee distributed in a smaller range and the cognitions are mostly consistent. It is the same as evaluating a person. No matter how many people evaluate him, the real evaluation (effective feedback trust degree) is mostly consistent. Theoretically, more credible of the evaluation (credibility) which is closer to true character. Therefore, the credibility of which feedback degree is closer the FTD_0 should be higher, and should be given larger weight.

Giving symmetric weight to feedback trust degree [23] could better satisfy the requirements above. Reference [23, 24] provide some weight vector which match the symmetry condition in order to use in practice. Such as: $\boldsymbol{\omega} = (\omega_1, \omega_2, \dots, \omega_m)^T$ is the weight vector and when:

$$\omega_i = \frac{e^{\frac{-\left(i-\frac{1+m}{2}\right)^2}{2\sigma_m^2}}}{\sum_{j=1}^{m} e^{\frac{-\left(j-\frac{1+m}{2}\right)^2}{2\sigma_m^2}}}, \quad \sigma_m^2 = \frac{1}{m}\sum_{i=1}^{m}\left(i - \frac{1+m}{2}\right)^2,$$

$$i = 1,2, \dots, m \quad (15)$$

$\boldsymbol{\omega}$ is symmetrical and $0 < \omega_i \leq 1$ $(i = 1, 2, \dots, m)$, $\sum_{i=1}^{m} \omega_i = 1$. When $m = 7$, the symmetric weight vector is:

$$\boldsymbol{\omega} = (0.0702, 0.1311, 0.1907, 0.2160, 0.1907, 0.1311, 0.0702)^T \quad (16)$$

Different symmetric weights have different influence on the result of the aggregation. But as a whole, the trend will not change after aggregation. If m feedback trust degree range in the interval of $[FTD_L, FTD_U]$ are asymmetry, it should do the normalization for corresponding weight.

2) Determine the Weight According to the Trust Degree From P_i to e_k

Experience tells us that people are always willing to believe the information provided by more credible person no matter what the information is. Specific to the feedback trust degree, higher the trust degree P_i to e_k is, more attention would be pay on the feedback information of provided by e_k. Therefore, the feedback information of e_k should be given greater weight, on the contrary, the feedback information provided by e_k with relative low trust degree should be given smaller weight. Show effective feedback trust degree in the form of binary group $\left(DT(P_i, e_k), FTD(P_i, P_j, e_k)\right)$ $(k = 1,2, \dots, m)$, abbreviated as $\left(DT_{ik}, FTD_{ij}^{(k)}\right)$ $(k = 1,2, \dots, m)$, then assign the weight for $FTD_{ij}^{(k)}$ according to the value of DT_{ik} .

Variable weight comprehensive analysis method [25] is one of the weight analysis method of factor space theory and knowledge representation. Improve the influence of feedback information of FR with higher trust degree on the comprehensive evaluation by means of the motivation of mixed variable weight method. Punish the feedback information of FR with low trust degree to minimize the influence on the comprehensive evaluation result. To a certain extent, it reflects the thought of "praising virtue and punishing vice".

The basic principle and strict mathematical discussion of variable weight method can consult relevant reference [25, 26]. Reference [27] presents a compromise type variable weight method that motivate the broader factors pointed to the defect of hybrid variable weight which is only incentive a specific factors. And the compromise type variable weight is:

$$w_k(\boldsymbol{x}) = \frac{w_k^{(0)} u_k'(x_k)}{\sum_{j=1}^{m} w_j^{(0)} u_j'(x_j)} \quad (17)$$

$w_k^{(0)} \in [0,1]$, $\sum_{k=1}^{m} w_k^{(0)} = 1$is the constant weight; $\boldsymbol{x} = (x_1, x_2, \dots, x_m)$ is the weight factor value vector ; Balanced function $u_k(x)\ (k = 1,2, \dots, m)$ is for punish - incentive effect, and it is a second order differentiable function. When $u_k''(x) < 0$, $u_k(x)$ is for punish effect; When $u_k''(x) > 0$, $u_k(x)$ is for the incentive effect; When $u_k''(x) = 0$, $u_k(x)$ is neutral (or constant). Here is an instance of compromise of the type variable weight function:

$$u_k(x_k) = \frac{1}{6}x_k^3 - \frac{1}{2}p_k x_k^2 + \left(\frac{5}{6} + \frac{1}{2}p_k\right)x_k \quad (18)$$

$\boldsymbol{p} = (p_1, p_2, \dots, p_m)^T$ is constant vector, known as the qualified level. p_k is the "qualifying level" or "general requirements" of kth factor. In essence, incentivize when it is higher than the level, punish when it is low than the level.

Take the derivative of formula (18), then substitute into formula (17), compromise type variable weight can be obtained:

$$w_k(\boldsymbol{x}) = \frac{w_k^{(0)}\left(\frac{1}{2}x_k^2 - p_k x_k + \left(\frac{5}{6} + \frac{1}{2}p_k\right)\right)}{\sum_{j=1}^{m} w_j^{(0)}\left(\frac{1}{2}x_j^2 - p_j x_j + \left(\frac{5}{6} + \frac{1}{2}p_j\right)\right)} \quad (19)$$

Under the control of constant weights vector $w^{(0)} = (w_1^{(0)}, w_2^{(0)}, \dots, w_m^{(0)})$, if a qualify level p has been given, adjustment with punishment or incentive will be done. p can be a constant value or a interval value. $p_k\ (k = 1,2, \dots, m)$ could be the same or different. For example, assuming $p_1 = p_2 = \cdots = p_m = 0.5$, when $x_k \geq 0.5$, the weight determined by the formula (19) is larger (incentive weight), on the other hand, when $x_k \leq 0.5$, w_k is smaller (punishment weight). For more example, when $p_k \in [0.5,0.7]\ (k = 1,2, \dots, m)$, it shows that FTD corresponding to lower $x_k (x_k \leq 0.5)$ would get punish weights, the FTD corresponding to larger $x_k (x_k \geq 0.7)$ would get incentive weights. The FTD corresponding to the weight within the range do not be adjusted. In the formula (19), $x_k\ (k = 1,2, \dots, m)$ is the direct trust degree $DT(P_i, e_k)(k = 1,2, \dots, m)$ trust subject P_i to the FR entitye_k.

Using the variable weight comprehensive evaluate method embodies the weights of feedback trust degree $FTD(P_i, P_j, e_k)\ (k = 1,2, \dots, m)$ of each FR entities $e_k\ (k = 1,2, \dots, m)$ changed with $DT(P_i, e_k)(k = 1,2, \dots, m)$, and it could incentive or punish the part of the feedback information. This method itself and its clear division for different feedback trust degree show the trust degree from Trustor to different feedback information of FR entity. It makes the aggregation of feedback trust degree more reasonable.

Above is the understanding of trust relationship from different aspects. All above is conformed to the actual life experience of human beings. It reflects the comprehensive understanding of trust. In the 4th part of this paper, two cases have been compared by two instances.

3.4. The Computation Overall Trust Degree

Overall trust degree is a function of direct trust degree and feedback trust degree. It can be represented as:

$$OTD_{ij} = v_1 \times DT_{ij} + v_2 \times g_{k=1}^{m}\left(FTD_{ij}^{k}\right) \quad (20)$$

OTD_{ij} is the abbreviation of $OTD(P_i, P_j)$. It is the weight sum of direct trust degreeDT_{ij} and aggregation feedback trust degree $g_{k=1}^{m}\left(FTD_{ij}^{k}\right)$. v_1 and v_2 are weights of DT_{ij} and $g_{k=1}^{m}\left(FTD_{ij}^{k}\right)$.

When calculating the overall trust degree, following issues should be taken into account:

1) People always believe in their own judgment at first, only when they are confused, they need to take others' feedback information for reference. Therefore, the weight of direct trust degree should not less than the weight of feedback trust degree.
2) People always value their long-term trust relationship with others which have already built up. Therefore, in the long-term interaction, the more successful interactions is, the larger trust degree is.
3) During the trust evaluation, the more positive feedback information, is, the more credible trust relationship is. Therefore, the more effective feedback entities means the feedback trust is more credible.

Pointing at the second problem, this paper defines motivating factor to make a description.

Definition 9 Motivating Factor

Assuming the Trustor and the Trustee had H interactions, h times of that are successful, then motivating factor is defined as: $\varepsilon = h/H$.

Pointing at the third problem, this paper defines feedback factor to make a description.

Definition 10 Feedback Factor

Assuming there are M feedback entities feedback Trustee's trust degree for Trustor. The feedback information of, m feedback entities is accepted by the Trustor, then feedback factor is defined as: $\theta = m/M$.

Motivating factor and feedback factor describe the trust degree of Trustee from different aspects.

Definition 11 Entity Active Degree

Entity Active Degree represents activity degree of Trustee in the open network environment. Higher activity degree suggests that interactions between Trustee and Trustor are more, and the Trustee is more credible. Theentity active degree of trustee is defined as:

$$\tau = \frac{\varepsilon + \theta}{2 + \delta} \quad (21)$$

Formula (21) shows that higher the motivating factor ε and the feedback factor $\theta$are, higher the entity active degree is. δ is regulatory factor, a non negative, which is determined by the values of ε and θ. The value of v_1 and v_2 in formula (22) will be explained later. Because $\varepsilon, \theta \in [0,1]$, then

$\tau \in [0,1]$. For instants, when $\varepsilon = 0.9$, $\theta = 0.6$, $\delta = 0.2$, it can calculate $\tau = 0.682$.

According to the parameters above, the weight coefficient v_1 and v_2 in formula (20) are defined as:

$$v_1 = \frac{1}{1+\tau}, \quad v_2 = \frac{\tau}{1+\tau} \tag{22}$$

Obviously, $v_1, v_2 \in [0,1]$, $v_1 + v_2 = 1$.And because of $\tau \in [0,1]$, v_1 is not less than v_2 (to assure the requirements of question 1 above).In the last case,$\tau = 0.682$,, and the result of calculation is $v_1 = 0.59$, $v_2 = 0.41$.Though the formula (21) and formula (22), it can be found that greater the adjustment factor δ is, larger the weight of direct trust degreev_1 is, and smaller the weight of feedback trust degree is. The recognition degree of Trustor to the direct trust degree of Trustee is presented through the value of δ.

Finally, the overall trust degree calculation formula is given by integrating the above analysis:

$$OTD_{ij} = \begin{cases} v_1 \times DT_{ij} + v_2 \times g_{k=1}^{m}\left(FTD_{ij}^{k}\right) \alpha \leq DT_{ij} < \beta \\ DT_{ij} DT_{ij} < \alpha \text{ or } DT_{ij} \geq \beta \end{cases} \tag{23}$$

$\alpha$is the trust threshold, β is the direct trust threshold.

4. EXAMPLE VERIFICATION

This section makes validity verification for overall trust degree prediction model proposed in this chapter by an instance. Trustor (P_i) is a computer which provide FTP service with service hierarchy, and it specifies the different service access to satisfy the Trustee which have different trust degree requirements. Trustee (P_j) is a computer which request service. FR entities are 11 computers, namely e_1~e_{11}.

Security policy specifies the trust threshold$\alpha = 0.3$, the direct trust threshold $\beta = 0.9$.The evaluation of trust degree in the recent 10 interactions from P_i to P_j is:

DT = {0.7564,0.8059,0.8123,0.7653,0.9234,

0.8965,0.9122,0.9273,0.7796,0.8637}

Select orness measures level α is 10/27, according to the formula (5), weight sequence {0.04, 0.05, 0.06, 0.04, 0.05, 0.11, 0.12, 0.14, 0.15, 0.16} could be got. Make an aggregation for10 historical data according to the formula (4), the results is 0.8568, namely$DT_{ij} = 0.8568$. Then$\alpha < DT_{ij} < \beta$, $P_i$need to get feedback information for trust evaluation onP_j.

Direct trust degree of P_i to 11 FR entities e_1~e_{11}, and direct trust degree of P_i, and the feedback trust degree $FTD(P_i, P_j, e_k)$ calculated by formula (8), as shown in Table **1**.

After use non-statistical distribution method to estimate the feedback trust degree in Table **1**, we get the result as follows: $FTD_0 = 0.7390$, $FTD_L = 0.63285$, $FTD_U = 0.89661$. Therefore, the effective feedback trust degree can be accepted by P_i are: 0.6720, 0.8124, 0.8254, 0.7845,

Table 1. The Instance of $DT(P_i, e_k)$、$DT(e_k, P_j)$ and $FTD(P_i, P_j, e_k)$.

k	1	2	3
$DT(P_i, e_k)$	0.7200	0.7532	0.8966
$DT(e_k, P_j)$	0.6378	0.8922	0.5431
$FTD(P_i, P_j, e_k)$	0.4592	0.6720	0.4869
k	4	5	6
$DT(P_i, e_k)$	0.8854	0.9231	0.7704
$DT(e_k, P_j)$	0.9175	0.8942	0.8127
$FTD(P_i, P_j, e_k)$	0.8124	0.8254	0.6261
k	7	8	9
$DT(P_i, e_k)$	0.8128	0.9057	0.8493
$DT(e_k, P_j)$	0.7359	0.8662	0.7683
$FTD(P_i, P_j, e_k)$	0.5981	0.7845	0.6525
k	10	11	/
$DT(P_i, e_k)$	0.8961	0.7941	/
$DT(e_k, P_j)$	0.7749	0.8053	/
$FTD(P_i, P_j, e_k)$	0.6944	0.6395	/

0.6525, 0.6944, 0.6525, a total of 7. Now we use two kinds of method introduced in section 3.3 to aggregate feedback trust degree.

1) Calculate the feedback trust degree by Symmetric weight method. Determine the weight in accordance with formula (16), as shown in Table **2**.

Substitute the feedback trust degree of table 2 and the corresponding weight into formula (14), and the results of aggregation is:

$$g_{k=1}^{7}\left(FTD_{ij}^{k}\right) = 0.7226 \quad (24)$$

2) Using compromise type variable weight method in aggregation of feedback trust degree. Variable weight formula is formula (19). For the sake of simplicity, assuming $w_k^{(0)} = 1/7$, $p_k = 0.5$ $(k = 1,2,\ldots,7)$. It can be known from the table 1 that the corresponding binary group are (0.7532, 0.7532), (0.8854, 0.8854), (0.9231, 0.9231), (0.9057, 0.9057), (0.8493, 0.8493), (0.8961, 0.8961), (0.7941, 0.7941). The weight after calculation is shown in Table **3**.

Substitute the result into formula (14), the aggregation results of feedback trust degree is:

$$g_{k=1}^{7}\left(FTD_{ij}^{k}\right) = 0.7269 \quad (25)$$

Compare formula (24) with formula (25), it could be found that use two weight determining methods on the same set of feedback trust degree the results are almost equal. Of course, it is the expected result. Because the two methods are all fit with the nature features of the trust relationship judging. Although the angle of viewing is different, the result is similar.

In addition, it could be found the aggregation of feedback trust degree distribute around of FTD_0, which we are expected, would not deviate too far, because it is determined by the essential characteristic of trust relationship.

Then, then calculate the overall trust degree from the results in the section 3.5 $v_1 = 0.59$, $v_2 = 0.41$:

$$OTD_{ij} = 0.59\times0.8568 + 0.41\times0.7226 = 0.8018$$

(Use the results of formula (24))

$$OTD_{ij} = 0.59\times0.8568 + 0.41\times0.7269 = 0.8035$$

(Use the results of formula (25))

Based on the same direct trust degree and the similar feedback trust degree, the overall trust degree P_i to P_j would not have too much difference. It could be assigned with appropriate authority distributions according to the definition of certain security policy and the trust degree from P_i to P_j.

CONCLUSION

The establishment of trust relationship between entities provides the credibility of their interaction. Although the trust relationship cannot replace the security relationship completely, it can still avoid some potential threatens caused by blind interact of entities. The model proposed in this paper following characteristics:

1) This paper presents the technical routine of the dynamic trust relationship prediction model, and brings the trust relationship under different condition into an entire system, which makes the trust relationship easier to be hold on the whole.
2) This model can identify the malicious recommendations and error recommendations, and eliminate their harmful influences on the trust relationship judgment. It could make the result more efficient.
3) This model emphasizes the importance of direct trust degree and pays much attention on the direct trust degree, which meets the experience of sociology.
4) This model takes fuzzy weights to incentives or penalties the trust degree. It fully embodies the importance of weights to the dynamic of the model, and reflects the essential characteristic of the trust relationships between entities.

Table 2. The weight of feedback trust degree (symmetric weight method).

$FTD(P_i, P_j, e_k)$	0.6395	0.6525	0.6720	0.6944
w_k	0.0702	0.1311	0.1907	0.2160
$FTD(P_i, P_j, e_k)$	0.7845	0.8124	0.8254	/
w_k	0.1907	0.1311	0.0702	/

Table 3. The weight of feedback trust degree (variable weight method).

$FTD(P_i, P_j, e_k)$	0.6720	0.8124	0.8254	0.7845
w_k	0.1381	0.1440	0.1462	0.1452
$FTD(P_i, P_j, e_k)$	0.6525	0.6944	0.6395	/
w_k	0.1422	0.1446	0.1397	/

5) This model solves the three problems proposed firstly in this paper well, especially the problem of sample size. This model does not have any requirements to sample size and the sample distribution. It integrates the scattered trust degree data regularly, and aggregates the direct trust degree and feedback trust degree reasonably.

The dynamic trust relationship prediction model proposed in this paper is built on a better understanding of the essence of trust relationship. Fuzzy weight reflects the dynamics and complexity of all kinds of trust relationship on the basis of historical certain information. This model do not contain complicated calculation, and every algorithm in this model has good convergence and extensibility.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," In*: Proceedings of the 1996 IEEE Symposium on Security and Privacy*, Washington: IEEE Computer Society Press, 1996, pp. 164-173.

[2] T. Mayayise, and O. Olusegun, "E-Commerce assurance models and trustworthiness issues: An empirical study," *Journal of Information Management & Computer Security*, vol. 22, pp. 76-96, 2014.

[3] M. Hoogendoorn, S.W. Jaffry, P.P. van Maanen, and J. Treur, "Design and validation of a relative trust model," *Knowledge-Based Systems (KBS)*, vol. 57, pp. 81-94, 2014.

[4] Y. Wang, X. Wang, and W. Zuo, "Trust prediction modeling based on social theories," *Journal of Software*, vol. 25, pp. 2893-2904, 2014. (in Chinese with English abstract)

[5] K. Shao, F. Luo, N. Mei, and Z.T. Liu, "Normal distribution based dynamical recommendation trust model," *Journal of Software*, vol. 23, pp. 3130-3148, 2012. (in Chinese with English abstract).

[6] F. Almenarez, A. Marin, D. Diaz, and J. Sanchez, "Developing a model for trust management in pervasive devices," In: *Bob Werner, Ed. Proceedings of the 3rd IEEE International Workshop on Pervasive Computing and Communication Security*, Washington: IEEE Computer Society Press, 2006, pp. 267-272.

[7] F. Almenarez, A. Marin, C. Campo, and R.C. Garcia, "PTM: A pervasive trust management model for dynamic open environments," In: *Proceedings of the 1st Workshop on Pervasive Security, Privacy and Trust*, Boston, 2004.

[8] H. Jameel, L.X. Hung, U. Kalim, A. Asjjad, S.Y. Lee, and Y.K. Lee, "A trust model for ubiquitous systems based on vectors of trust values," In: *Proceedings of the 7th IEEE International Symposum on Multimedia*, Washington, IEEE Computer Society Press, 2005, pp. 674-679.

[9] G. Theodorakopoulos, and J.S. Baras, "On trust models and trust evaluation metrics for ad-hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 318-328, 2006.

[10] Y. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Information theoretic framework of trust modeling and evaluation for an-hoc networks," *IEEE Journal on Selected Areas in Communications. Selected Areas in Communications*, vol. 249, pp. 305-319, 2006.

[11] Y. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Trust modelling and evaluation in ad-hoc networks," In: *Proceedings of the Global Telecommunications Conference*, Globecom 2005. Washington: IEEE Computer Society Press, 2005, pp. 1-10.

[12] R. He, J.W. Niu, and G.W. Zhang, "*CBTM: A Trust Model with Uncertainty Quantification and Reasoning for Pervasive Computing*," LNCS 3758, Berlin: Springer-Verlag, 2005, pp. 541-552.

[13] D. Melaye, and Y. Demazeau, "*Bayesian Dynamic Trust Model*," LNCS 3690, Berlin: Springer-Verlag, 2005, pp. 480-489.

[14] C. Duma, and N. Shahmehri, "Dynamic trust metrics for peer-to-peer system," In: *Proceedings of the 16th International Workshop on Database and Expert Systems Applications*, Washington: IEEE Computer Society Press, 2005, pp. 776-781.

[15] K. Shao, F. Luo, N.X. Mei, and Z.T. Liu, "Normal distribution based dynamical recommendation trust model," *Journal of Software*, vol. 23, pp. 3130-3148, 2012. (in Chinese with English abstract)

[16] S.S. Song, K. Hwang, and M. Macwan, "Fuzzy trust integration for security enforcement in grid computing," In: *Proceedings of the International Symposium on Network and Parallel Computing (NPC 2004)*, LNCS 3222, Berlin: Springer-Verlag, 2005, pp. 9-21.

[17] W. Tang, and Z. Chen, "Research of subjective trust management model based on the fuzzy set theory," *Journal of Software*, vol. 14, pp. 1401-1408, 2003. (in Chinese with English abstract)

[18] F.J. Yu, H.G. Zhang, and F. Yan, "A fuzzy relation trust model in P2P system," In: *Proceeding of the 2006 International Conference on Computational Intelligence and Security (CIS'2006) Part 2*, IEEE Press, 2006, pp. 1497-1502.

[19] R. Fullér, and P. Majlender, "On obtaining minimal variability OWA operator weights," *Fuzzy Sets and Systems*, vol. 136, pp. 203-215, 2003.

[20] Z.S. Xu, "*Multiple-Period MAGDM Under Linguistic Assessments*," Technical Report, 2007.

[21] X. Xia, and Z. Wang, "A novel non-statistical theory and its applications to hypothesis testing,"*Acta Metrologica Sinica*, vol. 27, pp. 190-195, 2006. (in Chinese with English abstract)

[22] X.T. Xia, Z.Y. Wang, and Y.S. Gao, "Estimation of non-statistical uncertainty using fuzzy-set theory," *Measurement Science and Technology*, vol. 11, pp. 430-435, 2000. (in Chinese with English abstract)

[23] H. Zhang, and Z. Xu, "Study on the symmetry properties of weighting vectors of information aggregation operators," *Systems Engineering-Theory & Practice*, vol. 26, pp. 75-82, 2006. (in Chinese with English abstract)

[24] Z.S. Xu, "An overview of methods for determining OWA weights," *International Journal of Intelligent Systems*, vol. 20, pp. 843-865, 2005.

[25] H. Li, "Factor spaces and mathematical frame of knowledge representation (VIII)- variable weights analysis," *Fuzzy Systems and Mathematics*, vol. 9, pp. 1-9, 1995. (in Chinese with English abstract)

[26] H. Li, "Factor spaces and mathematical frame of knowledge representation (IX)- structure of balance functions and weber-fechner characteristics," *Fuzzy Systems and Mathematics*, vol. 10, pp. 12-19, 1995. (in Chinese with English abstract)

[27] W. Liu, "The penalty-incentive utility in variable weight synthesizing," *Systems Engineering-Theory & Practice*, 1998, pp. 41-47. (in Chinese with English abstract)

Received: June 10, 2015 Revised: July 29, 2015 Accepted: August 15, 2015